IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application No.:	09/938,944	§	
		§	Examiner: Shaw, Peling A.
Filed:	August 24, 2001	§	Group/Art Unit: 2144
		§	Atty. Dkt. No: 5181-82200
Inventor(s):		§	
Tran		§	
		§	
		§	
Title:	SYSTEM AND METHOD FOR CONTROLLING UNIX GROUP ACCESS USING LDAP	§	

****CERTIFICATE OF E-FILING TRANSMISSION****

I hereby certify that this correspondence is being transmitted via electronic filing to the United States Patent and Trademark Office on the date shown below

B. Noël Kivlin

Signature — January 15, 2008 — Date

APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir/Madam:

Further to the Notice of Appeal filed August 8, 2007, Appellants present this Appeal Brief. Appellants respectfully request that this appeal be considered by the Board of Patent Appeals and Interferences.

I. REAL PARTY IN INTEREST

As evidenced by the assignment recorded at Reel/Frame 012128/0182, the subject application is owned by Sun Microsystems, Inc., a corporation organized and existing under and by virtue of the laws of the State of Delaware, and now having its principal place of business at 4150 Network Circle, Santa Clara, CA 95054.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences known to Appellants, Appellants' legal representatives, or assignee which will directly affect, be directly affected by, or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1-25 are pending. Claims 1-25 are rejected, and the rejection of these claims is being appealed. A copy of claims 1-25 is included in the Claims Appendix attached hereto.

IV. STATUS OF AMENDMENTS

No amendments to the claims have been submitted subsequent to the final rejection.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 is directed to a method comprising populating a directory (see, e.g., FIG. 5, reference numeral 113; FIG. 6, reference numeral 601; page 3, lines 9 – 22; page 10, line 21 – page 12, line 21; page 13, lines 7 – 20) with entries (see, e.g., FIG. 5, reference numeral 502; page 10, line 28 – page 12, line 21) for each of a plurality of users (see, e.g., FIG. 4, reference numerals 402, 404, 406; page 10, lines 15 – 18) of a multi-user computing environment (see, e.g., FIG. 3, reference numeral 200; page 8, line 1 – page 9, line 19), wherein each entry in the directory comprises a user ID and one or more group names, wherein each of the one or more group names corresponds to a group to which the user ID belongs, and wherein at least one of the entries in the directory comprises a first group name of the one or more group names; determining a first group access control list (see, e.g., FIG. 5, reference numeral 127; FIG. 6, reference numeral 603; page 3, line 24 – page 4, line 2; page 12, lines 23 – 28; page 13, lines 22 – 29) for the first group name, wherein the first group access control list comprises the user IDs of users whose entries comprise the first group name, and wherein the first group access control list is stored outside of the directory; and, for each data source (see, e.g., FIG. 4, reference numeral 130; page 10, lines 5 – 7) in the multi-user computing environment which permits access by the first group name, granting access (see, e.g., FIG. 6, reference numeral 605; page 4, lines 4 – 13; page 14, lines 2 – 10) to the respective data source to the users in the first group access control list.

Independent claim 10 is directed to a system comprising a file system (see, e.g., FIG. 4, reference numeral 125; page 9, line 22 – page 10, line 7) which comprises one or more data sources (see, e.g., FIG. 4, reference numeral 130; page 10, lines 5 – 7) including a first data source; a directory server (see, e.g., FIG. 5, reference numeral 113; page 10, line 21 – page 12, line 21) which is configured to store a plurality of entries (see, e.g., FIG. 5, reference numeral 502; FIG. 6, reference numeral 601; page 3, lines 9 – 22; page 10, line 21 – page 12, line 21; page 13, lines 7 – 20) in a directory for a plurality of users (see, e.g., FIG. 4, reference numerals 402, 404, 406; page 10, lines 15 – 18), wherein each entry comprises a user ID and one or more group names which denote

groups to which the user ID belongs, wherein at least one of the entries comprises a first group name of the one or more group names; and a first group access control list (see, e.g., FIG. 5, reference numeral 127; page 12, lines 23 – 28) which is generated from the entries (see, e.g., FIG. 6, reference numeral 603; page 3, line 24 – page 4, line 2; page 13, lines 22 – 29), wherein the first group access control list is stored in the file system outside of the directory server, wherein the first group access control list comprises the at least one user IDs belonging to the first group name, and wherein the first group access control list is usable to permit access (see, e.g., FIG. 6, reference numeral 605; page 4, lines 4 – 13; page 14, lines 2 – 10) to the first data source to user IDs belonging to the first group name.

Independent claim 17 is directed to a computer-readable storage medium comprising program instructions (see, e.g., FIG. 1, reference numeral 110; page 6, lines 8 – 10 and 18 – 21) which are computer-executable (see, e.g., FIG. 1, reference numeral 102; FIG. 2, reference numeral 122; page 6, lines 8 – 10 and 18 – 21) to implement populating a directory (see, e.g., FIG. 5, reference numeral 113; FIG. 6, reference numeral 601; page 3, lines 9 – 22; page 10, line 21 – page 12, line 21; page 13, lines 7 – 20) with entries (see, e.g., FIG. 5, reference numeral 502; page 10, line 28 – page 12, line 21) for each of a plurality of users (see, e.g., FIG. 4, reference numerals 402, 404, 406; page 10, lines 15 – 18) of a multi-user computing environment (see, e.g., FIG. 3, reference numeral 200; page 8, line 1 – page 9, line 19), wherein each entry in the directory comprises a user ID and one or more group names, wherein each of the one or more group names corresponds to a group to which the user ID belongs, and wherein at least one of the entries in the directory comprises a first group name of the one or more group names; determining a first group access control list (see, e.g., FIG. 5, reference numeral 127; FIG. 6, reference numeral 603; page 3, line 24 – page 4, line 2; page 12, lines 23 – 28; page 13, lines 22 – 29) for the first group name, wherein the first group access control list comprises the user IDs of users whose entries comprise the first group name, and wherein the first group access control list is stored outside of the directory; and, for each data source (see, e.g., FIG. 4, reference numeral 130; page 10, lines 5 – 7) in the multi-user computing environment which permits access by the first group name,

granting access (see, e.g., FIG. 6, reference numeral 605; page 4, lines 4 – 13; page 14, lines 2 – 10) to the respective data source to the users in the first group access control list.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1-25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Shandony (U.S. Patent No. 6,675,261) in view of Mangat, et al. (U.S. Patent No. 6,049,799, hereinafter "Mangat").

VII. ARGUMENT

First Ground of Rejection:

Claims 1-25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Shandony (U.S. Patent No. 6,675,261) in view of Mangat, et al. (U.S. Patent No. 6,049,799, hereinafter "Mangat"). Appellants traverse this rejection for the following reasons. Different groups of claims are addressed under their respective subheadings.

Claims 1, 2, 4 – 11, 13 – 18, and 20 – 25:

Appellants respectfully submit that Shandony and Mangat, taken individually or in combination, do not teach or suggest that a first group access control list (comprising the user IDs of users whose entries comprise the first group name) is stored outside of the directory, in combination with the remaining features of claim 1.

The Final Office Action contends that Mangat teaches or suggests these features (in particular, at Figures 4 and 5; col. 2, lines 14-28; col. 12, lines 23-33; and col. 16, lines 13-21). Appellants respectfully disagree. Mangat discloses a method and apparatus for maintaining, updating, finding, and re-making links between documents and

consumers of those documents. Mangat also discloses a data structure created and maintained outside a directory services system for storing information about the documents. At various locations (e.g., Figure 5; col. 2, lines 14-28; and col. 16, lines 40-52), for example, Mangat discloses a data structure called a Docloc object which is usable for storing document information outside a directory services system. As shown in Figure 6, a Docloc object stores the title, language, version, description, doc file name, docloc table path, doc publication style, doc file types, doc security, fall back docloc object d.n., and object class for a document.

However, Mangat does not teach or suggest an access control list stored outside of the directory. To the contrary, Mangat discloses that all the elements that might be considered analogous to an access control list – namely, the group object (120), membership list (124), association lists (118, 136), and access rights (116, 122, 134) – are stored within the directory services server (60) (see, e.g., Figures 2-5). Mangat thus teaches away from Appellants' claimed invention. Accordingly, Appellants respectfully submit that Mangat does not teach or suggest the feature "wherein the first group access control list is stored outside of the directory" in combination with the remaining features of claim 1.

Shandony also fails to teach or suggest the feature "wherein the first group access control list is stored outside of the directory" in combination with the remaining features of claim 1. At various locations (e.g., col. 7, line 64 to col. 8, line 29), Shandony discloses a group manager (44) which permits the modification of access privileges for groups. In Figure 1, the group manager is depicted as being part of an identity server (40) which is external to a directory server (36). However, Shandony does not teach or suggest that any data structure modified by the group manager is stored outside of the directory. To the contrary, Shandony's identity server essentially provides a user interface for modification of data stored in the directory server. Therefore, there is nothing in Shandony to teach or suggest that a group access control list is stored outside of a directory.

In order to establish a prima facie obviousness of a claimed invention, all claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 U.S.P.Q. 580 (C.C.P.A. 1974), MPEP 2143.03. Obviousness cannot be established by combining or modifying the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion or incentive to do so. *In re Bond*, 910 F. 2d 81, 834, 15 USPQ2d 1566, 1568 (Fed. Cir. 1990). The Final Office Action asserts that the motivation for one of ordinary skill in the art to combine Shandony and Mangat is "to have group access functions different from user access functions per Mangat and Shadony's teaching." As discussed above, neither Shandony nor Mangat teaches or suggests a group access control list stored outside of a directory. Therefore, Appellants can find no basis in the cited art for the motivation asserted in the Final Office Action. The art cited by the Final Office Action does not, either singly or in combination, teach or suggest all limitations of the currently pending claim 1.

Accordingly, claim 1 and its dependent claims 2 and 4-9 are believed to patentably distinguish over the cited references for at least the reasons given above. Claims 10 and 17 recite features similar to those of claim 1 and are therefore believed to patentably distinguish over Shandony and Mangat for at least the reasons given above. Dependent claims 11, 13-16, 18, and 20-25 are also believed to patentably distinguish over the art cited by the Final Office Action for similar reasons.

Claims 3, 12, and 19:

Claim 3 depends on claim 1 and is therefore also believed to patentably distinguish over the art cited by the Final Office Action for the reasons given above. In addition, claim 3 recites a limitation "for each data source in the multi-user computing environment which permits access by the first hostname, granting access to the data source to the one or more users whose directory entries comprise the first hostname and who are seeking access from the host having the first hostname." None of the art cited by the Final Office Action, either singly or in combination, teaches or suggests such a limitation. Although Shandony discloses a policy URL (Uniform Resource Locator) obtained from a directory entry (see,

e.g., Figure 69 and col. 70, line 60 to col. 71, line 47), and although a URL may include a hostname, Shandony does not teach or suggest granting access to the data source to the one or more users whose directory entries comprise the first hostname and who are seeking access from the host having the first hostname. Appellants therefore respectfully submit that claim 3 patentably distinguishes over the cited art.

Claims 12 and 19 recite features similar to those of claim 3 and are therefore believed to patentably distinguish over Shandony and Mangat for at least the reasons given above.

For the foregoing reasons, it is submitted that the Examiner's rejection of claims 1-25 was erroneous, and reversal of the decision is respectfully requested.

A Fee Authorization form in the amount of $500 was submitted October 24, 2005 to cover the fee for filing a previous Appeal Brief. Appellants request that the previously paid fee be applied to the fee for filing the present Appeal Brief pursuant to MPEP §1204.01. The Commissioner is authorized to charge any fees that may be due to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 50-1505/5181-82200/BNK.

Respectfully submitted,

B. Noël Kivlin
Reg. No. 33,929
ATTORNEY FOR APPELLANT(S)

Meyertons, Hood, Kivlin, Kowert and Goetzel, P.C.
P.O. Box 398
Austin, Texas 78767-0398
Phone: (512) 853-8800
Date: January 15, 2008

VIII. CLAIMS APPENDIX

The claims on appeal are as follows.

1. A method comprising:

populating a directory with entries for each of a plurality of users of a multi-user computing environment, wherein each entry in the directory comprises a user ID and one or more group names, wherein each of the one or more group names corresponds to a group to which the user ID belongs, and wherein at least one of the entries in the directory comprises a first group name of the one or more group names;

determining a first group access control list for the first group name, wherein the first group access control list comprises the user IDs of users whose entries comprise the first group name, and wherein the first group access control list is stored outside of the directory;

for each data source in the multi-user computing environment which permits access by the first group name, granting access to the respective data source to the users in the first group access control list.

2. The method of claim 1,

wherein each entry in the directory comprises a user password; and

wherein the method further comprises authenticating each user ID using the associated user password.

3. The method of claim 1,

wherein each entry in the directory comprises zero, one, or a plurality of hostnames;

wherein the directory comprises a first hostname; and

wherein the method further comprises:

for each data source in the multi-user computing environment which permits access by the first hostname, granting access to the data source to the one or more users whose directory entries comprise

the first hostname and who are seeking access from the host having the first hostname.

4. The method of claim 1,

wherein the data source comprises a file or a directory in a file system coupled to the multi-user computing environment.

5. The method of claim 1,

wherein the access comprises read access; and

wherein the granting access to the data source to the users in the first group access control list comprises permitting the users in the first group access control list to read the data source.

6. The method of claim 1,

wherein the access comprises write access; and

wherein the granting access to the data source to the users in the first group access control list comprises permitting the users in the first group access control list to write to the data source.

7. The method of claim 1,

wherein the access comprises execute access; and

wherein the granting access to the data source to the users in the first group access control list comprises permitting the users in the first group access control list to execute the data source.

8. The method of claim 1,

for each data source in the multi-user computing environment which permits access by the first group name and owner but denies access to others, denying access to the data source to users who are not in the first group access control list and who are not the owner of the data source.

9. The method of claim 1,

wherein the multi-user computing environment comprises a UNIX-based operating system.

10. A system comprising:

a file system which comprises one or more data sources including a first data source;

a directory server which is configured to store a plurality of entries in a directory for a plurality of users, wherein each entry comprises a user ID and one or more group names which denote groups to which the user ID belongs, wherein at least one of the entries comprises a first group name of the one or more group names; and

a first group access control list which is generated from the entries, wherein the first group access control list is stored in the file system outside of the directory server, wherein the first group access control list comprises the at least one user IDs belonging to the first group name, and wherein the first group access control list is usable to permit access to the first data source to user IDs belonging to the first group name.

11. The system of claim 10,

wherein each entry in the directory comprises a user password, wherein the user password is usable to authenticate the corresponding user ID for access to the one or more data sources.

12. The system of claim 10, further comprising:

a host computer system coupled to the file system;

wherein each entry in the directory comprises zero, one, or a plurality of host names such that the directory server comprises a first host name corresponding to the host computer system, and wherein access is granted to the first data sources to users seeking access from the host computer system.

13. The system of claim 10,
wherein the access to the first data source comprises read access.

14. The system of claim 10,
wherein the access to the first data source comprises write access.

15. The system of claim 10,
wherein the access to the first data source comprises execute access.

16. The system of claim 10, further comprising:
an operating system which is operable to restrict user access to the data sources in the file system.

17. A computer-readable storage medium comprising program instructions which are computer-executable to implement:
populating a directory with entries for each of a plurality of users of a multi-user computing environment, wherein each entry in the directory comprises a user ID and one or more group names, wherein each of the one or more group names corresponds to a group to which the user ID belongs, and wherein at least one of the entries in the directory comprises a first group name of the one or more group names;
determining a first group access control list for the first group name, wherein the first group access control list comprises the user IDs of users whose entries comprise the first group name, and wherein the first group access control list is stored outside of the directory;
for each data source in the multi-user computing environment which permits access by the first group name, granting access to the respective data source to the users in the first group access control list.

18. The computer-readable storage medium of claim 17,

wherein each entry in the directory comprises a user password; and

wherein the program instructions are further computer-executable to implement authenticating each user ID using the associated user password.

19. The computer-readable storage medium of claim 17,

wherein each entry in the directory comprises zero, one, or a plurality of hostnames;

wherein the directory comprises a first hostname; and

wherein the program instructions are further computer-executable to implement :

for each data source in the multi-user computing environment which permits access by the first hostname, granting access to the data source to the one or more users whose entries comprise the first hostname and who are seeking access from the host having the first hostname.

20. The computer-readable storage medium of claim 17,

wherein the data source comprises a file or a directory in a file system coupled to the multi-user computing environment.

21. The computer-readable storage medium of claim 17,

wherein the access comprises read access; and

wherein the granting access to the data source to the users in the first group access control list comprises permitting the users in the first group access control list to read the data source.

22. The computer-readable storage medium of claim 17,

wherein the access comprises write access; and

wherein the granting access to the data source to the users in the first group access control list comprises permitting the users in the first group access control list to write to the data source.

23. The computer-readable storage medium of claim 17,

wherein the access comprises execute access; and

wherein the granting access to the data source to the users in the first group access control list comprises permitting the users in the first group access control list to execute the data source.

24. The computer-readable storage medium of claim 17, wherein the program instructions are further computer-executable to implement:

for each data source in the multi-user computing environment which permits access by the first group name and owner but denies access to others, denying access to the data source to users who are not in the first group access control list and who are not the owner of the data source.

25. The computer-readable storage medium of claim 17,

wherein the multi-user computing environment comprises a UNIX-based operating system.

IX. EVIDENCE APPENDIX

No evidence submitted under 37 CFR §§ 1.130, 1.131, or 1.132 or otherwise entered by the Examiner is relied upon in this appeal.

X. RELATED PROCEEDINGS APPENDIX

There are no related proceedings known to Appellants, Appellants' legal representatives, or assignee which will directly affect, be directly affected by, or have a bearing on the Board's decision in the pending appeal.